Multi Scenariokaart: Digitale verstoring (bijvoorbeeld cyberverstoring)

GGD BRANDWEER Veiligheidsregio Kennemerland

Scenario omschrijving

Een digitaal incident is **complex** vanwege de verwevenheid van het digitale met het fysieke domein. Ook zijn de **gevolgen vaak langere tijd nog niet zichtbaar**. Maatschappelijke ontwrichting als gevolg van incidenten in het digitale domein wordt vaak gekenmerkt door een **razendsnelle verspreiding en meerdere cascade-effecten**. De crisis ontstaat met **weinig oog voor geografische grenzen**, is mogelijk langdurig en er bestaat **vaak lang onzekerheid over oorzaak, omvang en impact** (koepelnotitie NCTV).

Aandachtspunten:

Operationeel / Tactisch:

- Start zo snel mogelijk met diagnose: wat is geraakt, wat is de impact en welke maatregelen zijn prio's.
- Anders dan bij een fysieke crisis of incident, kan de oorzaak lang onduidelijk blijven. Het kan van alles zijn gezien de afhankelijkheid/complexiteit van systemen.
- Contact het NCC of LOCC voor duiding en informatiedeling getroffen systemen extern. Contact VRISAC/CISO voor duiding ten aanzien van eigen systemen en mogelijk crisisorganisatie.
- Gebruik Nationaal Crisisplan Digitaal (NCP-D) en bestuurlijke netwerkkaarten om de betrokken partijen te bepalen (zie links planvorming).

Nationaal Crisisplan Digitaal::

Stap 1 NCP-D: scenario(s) bepalen aan de hand van bouwstenen:

- Oorzaak: onbekend / opzettelijk / niet-opzettelijk
- Bron: binnen / buiten Nederland
- Geraakt domein: onbekend / digitaal / maatschappelijk belangrijk / vitaal
- Geraakt gebied: onbekend / 1 VR / meerdere VR
- Technisch oplossingsperspectief: onbekend / aanwezig / afwezig

Stap 2 NCP-D: per scenario de vragen beantwoorden:

1. Wat zijn de belangrijkste mogelijke (in)directe gevolgen en effecten?
2. Welke mitigerende maatregelen zijn nodig om de gevolgen en effecten te voorkomen of te beheersen?
3. Welke partijen zijn betrokken c.q. nodig voor een adequate aanpak?

Bestuurlijk:

- Duiding maatregelen technisch operationeel en handelingsperspectief voor eigen doelgroep/organisatie door NCSC, CERT- en SOC-organisaties - Duiding gevolgen nationale veiligheid en veiligheidsmaatregelen algemeen door NCTV (en/of MinJenV).
- Duiding en handelingsperspectief waar ICT-beveiliging voor nationale veiligheid van belang is (via NBV) door AIVD.

Bestuurlijke uitgangspunten/dilema's:

- Rol van het bestuur richting de maatschappij?
- Wanneer communiceer je over dreiging? Cyberdreiging kan snel escaleren naar crisis.
- Wat isoleer je door uit te schakelen en wat laat je aan? Wanneer besluit je om systemen weer aan te zetten zonder 100% garantie dat het veilig is?
- Forensische opsporing en monitoring vs continuïteit dienstverlening.
- Wel of niet betalen van ransomware? Afwegingen: imago, kosten, verlies van data/kritische processen.
- Uitgangspunten: zie handreiking cybergevolgbestrijding G4 + commander's intent.

Plannen en Procedures (ook te vinden door titel te zoeken in Google):

- Cyberscenario's voor veiligheidsregio's
- Nationaal Crisisplan Digitaal
- Handreiking Cybergevolgbestrijding (CGB): duiden verstoring en effecten, betrokken netwerk en checklist sleutelmomenten/sleutelbesluiten.
- Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring).
- Koepelnotitie Communicatie bij digitale incidenten 2021

Bestuurlijke netwerkkaarten en bevoegdhedenschema (IFV)

- Bestuurlijke netwerkkaart 21b: cybersecurity

Melden, alarmeren & Opschalen:

Intern incident (vb. ransomware veiligheidsregio)

- Informeer directie, FG, de CISO voor interne bedrijfsvoering
- Doe aangifte; overleg met (externe) systeembeheerder hoe/wat ontkoppeld moet worden.
- Afstemming tussen de CaCo en OL over de wijze van alarmeren en samenstelling team.
- Schaal flexibel op. Betrek: directie, jurist, FG, business controller, CISO en systeemverantwoordelijken.
- Overweeg twee teams: intern (diagnose en scenario's) en extern (crisisbeheersing en partners).

Extern incident (vb. hack bij regionale partner)

- Zie intern, en:
- Alarmeer conform bestaande plannen, maar kies initieel bij voorkeur voor heimelijk alarmeren (zonder P2000), zeker bij dreiging zonder zichtbare effecten/opsporingsonderzoek t.b.v. vertrouwelijkheid.
- Informeer omliggende regio's.

Leiding en Coördinatie:

- Digitale verstoringen zijn snel bovenregionaal/nationaal en bron is mogelijk lastig te duiden; het NCC is voor veiligheidsregio's het 24/7 informatieloket en contactpunt van het rijk en legt de verbinding met de andere ministeries en het NCSC, in nauwe samenwerking met het LOCC.
- Leg verbinding met Politie (en Kmar en OM) voor opsporingsexpertise.

Doelstellingen (Commander's intent):

- Continuïteit van de hulpverlening en de crisisorganisatie waarborgen.
- Inzichtelijk maken van zowel interne als externe effecten.
- Voorbereiden en inspelen op mogelijke effecten of dreiging daarvan.
- Prioriteit bepalen voor herstel interne processen.

Informatiemanagement:

- De Operationeel Leider, Informatiemanager (eventueel CaCo) stemmen af over het informatiemanagement.
- Check bij de partners naar behoefte om beeldvorming en knelpunten te delen.
- Initieer/check via LOCC een landelijk beeld en afstemming
- Uitval LCMS is onwaarschijnlijk en redundant uitgevoerd. Valt het wel uit: zie dan hoofdstuk 3.10, uitval LCMS, Continuïteitsplan VRK..

Crisiscommunicatie:

- Houdt vast aan bestaande structuren, rollen en werkwijzen.
- Bij een cyberdreiging/aanval in de woordvoering 'digitale verstoring' aanhouden, totdat het OM of het NCTV anders bepaalt.
- Nadruk op proces informatie; 'we doen er alles aan om de oorzaak te achterhalen / de verstoring te beperken / erger te voorkomen' en zo verder.
- Communicatierol NCTV (NKC) en Rijk is afhankelijk van maatschappelijke impact en uitstraling.
- Communicatiedilemma's: wie gaat er over. Ongrijpbaar door onduidelijke bron (tijdsduur, snelheid opsporing). Overzien welke informatie op straat komt te liggen. Beeld dat overheid ICT niet op orde heeft.

Nafase en herstel:

- Houdt rekening met een langdurig herstel (grote herstelwerkzaamheden tot een maand, overige storingen tot enkele maanden).
- Laat ICT-experts/CISO meedenken in het duiden en besluiten bij dilemma's (bijvoorbeeld: risico's voor het herstarten van systemen).

Contactgegevens/Checklist

NCSC	(070) 751 55 55
LOCC	088 662 80 48
NCC	(070) 751 54 00

Denk ook aan:

- Afdelingen binnen de VRK
- Vitale partners in de regio
- Functionaris gegevensbescherming
- Directie
- VR ISAC
- OM
- Politie
- OM
- KMar

Multi Scenariokaart: Digitale verstoring (bijvoorbeeld cyberverstoring)

GGD BRANDWEER Veiligheidsregio Kennemerland

Brandweer multidisciplinaire aandachtspunten

- Geen multi-relevante aanvullingen.

Bevolkingszorg / crisiscommunicatie multidisciplinaire aandachtspunten

Bevolkingzorg

- Afhankelijk van het effect van de cyberaanval op de bevolking bepalen of processen Publieke Zorg, Informeren Verwanten, Omgevingszorg en/of preparatie Nafase nodig zijn. Indien de cyberaanval effect heeft op één of meerdere gemeenten, deze goed betrekken op de benodigde niveaus.

Crisiscommunicatie

- Vergelijk het label 'cyberaanval' met het label 'terrorisme' dat alleen door het OM of het NCTV wordt bepaald.
- Afzender communicatie over impact hangt af van situatie. Dit kan beperkt zijn tot getroffen organisatie, maar ook meerdere betrokken/getroffen partijen betreffen.
- Grootste communicatieopgave bij een cyberincident ligt in de blauwe kolom: OM, politie/KMar en NCTV (Rijk, NCSC). Regio geeft geen technische duiding.
- Denk bij scenario's aan de eigen continuïteit. Gaat het communicatiemiddelen raken, gaan ze daardoor uitvallen of verstoren?
- Bij uitval mobiel netwerk blijft NL-Alert mogelijk.
- Stem inhoud en timing van boodschappen af met NKC (NCC/NCTV) om onrust door tegenstrijdigheden of onduidelijkheid te voorkomen. Er zijn verschillende opvattingen over begrippen en terminologieën. Het NCC staat in direct contact met het Nationaal Cyber Security Centrum (NCSC), de inhoudelijk specialisten.
- Zorg dat je iemand in je netwerk/taakorganisatie hebt die goed is in het vertalen van technische informatie naar 'lekentaal'. Zie cyberwoordenboek.

GHOR multidisciplinaire aandachtspunten

- Mogelijk effecten op zorgcontinuïteit bij ketenpartners waarbij ondersteuning van VRK nodig is of die gevolgen heeft voor de geneeskundige hulpverlening (denk aan opnamestops, stop op B-vervoer ambulances, uitval vitale infrastructuur met gevolgen voor de zorg etc.)
- Indien een crisis met (veel) slachtoffers samenvalt met de Cybercrisis: mogelijk incompleet of geen slachtofferbeeld

Politie multidisciplinaire aandachtspunten

- Geen multi-relevante aanvullingen.

Defensie multidisciplinaire aandachtspunten

- Geen multi-relevante aanvullingen.

Liaison X

Partij X

Geleerde lessen

- Ransomware VNOG: houdt rekening met sociaal-emotionele impact voor collega's. (VNOG)
- Landelijke 112-storing: vertrouw op improvisatievermogen en stem communicatie goed af. (112-storing)
- Ransomware Gemeente Hof van Twente: indien mogelijk, wees open en eerlijk over eigen verstoring. (Hof van Twente)

Scenario denken / Strategische analyse

Benut het scenario denken / de strategische analyse om vooruit in de tijd te kijken en hierop proactief te handelen.
Onderdelen hiervan zijn

- *Kernbeeld van de situatie nu*
- *Stel een gunstig en ongunstig scenario op middellang termijn 4 – 12 uur en > 12 uur.*
- *Escalerend of de-escalerend factoren t.o.v. scenario*
- *Benoem de doelgroep*
- *Welke dilemma's (wel of niet ingrijpen)*
- *Besluiten formuleren*

Ransomware intern (cyberscenario's IFV):

0-6 uur:

- Wat is geraakt? Wat voor effecten heeft dat? Welke besluiten moeten nu genomen worden? Gebruik hiervoor ook de bouwstenen uit het NCP-D
- Wordt er preventief geïnformeerd, intern en extern?
- Wanneer gaat men over tot alarmeren?

> 6 uur:

- Crisiscommunicatie: openheid versus geslotenheid?
- Hoe mobiliseer je externe expertise? Interne crisisorganisatie/opschaling
- GRIP-procedure
- Voor welke crisisstructuur kies je?
- Hoe mobiliseer je externe expertise? Wie ga je bellen?
- Welke afspraken zijn er met leveranciers?
- Welke interne collega's moet je betrekken?
- Wat is de samenstelling van de interne crisisorganisatie?
- Is er contact met VR-ISAC?
- Is er aangifte gedaan?
- Hoe organiseer je beslisbevoegdheid? Wie is bevoegd tot bijvoorbeeld het besluit inzake losgeld?
- Welke hulpmiddelen (plannen, draaiboeken) kan je benutten?

Hack regionale partner (cyberscenario's IFV):

0-6 uur:

- Wat is je informatiepositie?
- Welke rol voorzie je voor de veiligheidsregio?
- Hoe raak je als veiligheidsregio betrokken?
- Hoe verloopt het contact tussen veiligheidsregio's en bedrijf x?
- Is er contact tussen veiligheidsregio's?

> 6 uur:

- Ga je acteren op (dreigings)informatie vanuit het bedrijf?
- Ga je acteren op vertrouwelijke informatie? Mag/kan dat?
- Wie kan beoordelen of de oplossing van het bedrijf voldoende is?
- Speelt het probleem breder (bijv. ook bij andere (BRZO) bedrijven)?
- Wat zijn worst case en best case scenario's?
- Wanneer kies je voor GRIP?
- Neem je als veiligheidsregio extra maatregelen nu blijkt dat er mogelijkerwijs een cybercomponent is betrokken?

> 48 uur:

- Wat ga je als veiligheidsregio doen wanneer er verhoogde kans is dat andere vitale organisaties ook worden aangevallen?
- Wanneer ga je afschalen?

Achtergrondinformatie

Definities

Cyber: Iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het internet.
Cyberaanval: Een gerichte aanval in of via cyberspace. Doelwitten kunnen zijn: personen, groepen, bedrijven en organisaties, overheden, andere landen
Gijzelsoftware/ransomware: Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker.
(VR)ISAC: veiligheidsregio Information Sharing and Analysis Centre. Overleg over cybersecurity dat regelmatig plaatsvindt. Tijdens dit overleg delen organisaties uit dezelfde sector gevoelige informatie over beveiligingsincidenten, dreigingen, zwakke plekken en maatregelen op het gebied van cybersecurity. Doel hiervan is dat de organisaties van elkaar leren.
NCSC: nationaal cyber security centre; binnen het Nationaal Cyber Security Centrum worden tactische en operationele kennis zoals expertise, uit zowel publieke als private sectoren bij elkaar gebracht
FG: functionaris gegevensbescherming
CISO: Chief Information Security Officer
CERT: Computer Emergency Respons team
SOC: Security Operations Centre
NBV: Nationaal Bureau voor Verbindingsbeveiliging

Kwetsbare / vitale objecten

De aard van een cybercrisis is dat deze zich niet houdt aan grenzen van systemen, bedrijven, regio's of zelfs landen. In theorie kan ieder systeem en bedrijf getroffen worden door een cyberaanval. Gebruik voor inzichtelijk maken van kwetsbare/vitale objecten het regionaal risicoprofiel, LCMS plot of andere hulpmiddelen.

Zie ook de netwerkkaart in de handreiking cybergevolgbestrijding (warme fase). Pagina 5.

Specifieke informatie

Mogelijke rollen voor veiligheidsregio's (IFV):
Risicoadviseur: hoofdzakelijk in de koude fase, dialoog met bedrijven t.a.v. bewustwording.
Netwerkadviseur: partijen bij elkaar brengen voor risico- en scenarioanalyse.
Bijstandsverlener: faciliteren van een crisisstructuur of helpen bij crisiscommunicatie.
Probleemeigenaar: verantwoordelijk voor bron- en effectbestrijding als gevolg van de verstoring.
Gevolgbestrijder: bestrijden van (fysieke) gevolgen
Digitale brandweer: bron- en effectbestrijding van een externe cyberverstoring.